Listing of Claims:

The listing of claims replaces all prior versions, and listings, of claims in the application.

1. (Previously Presented) A method for authenticating a digital medium by determining the presence of an anomaly region corresponding to a data segment of the digital medium comprising:

performing multiple read operations on a data segment of the medium to generate multiple corresponding read data results;

calculating corresponding digital signatures using actual data values of underlying data of the read data segment for each of the multiple read data results;

determining whether an anomaly region is present in the data segment based on a comparison of the digital signatures by determining whether any of the digital signatures are equal in value, and if a predetermined number of the digital signatures are not equal in value, determining the anomaly region to be present; and

authenticating the medium in response to the determination of the presence of the anomaly region.

2. (Original) The method of claim 1 wherein the data comprises data selected from the group consisting of: user data, error data, sync data, parity data, header data, and sub-channel data.

3. (Original) The method of claim 1 further comprising monitoring a transfer rate of the read data during at least one of the read procedures, and further determining whether an anomaly region is present in the data segment based on the monitored transfer rate.

4. (Original) The method of claim 1 further comprising:

first monitoring a first transfer rate of first read data during one of the read procedures, and further determining whether an anomaly region is present in the data segment based on the monitored first transfer rate; and

in the event that the presence of an anomaly is not determined as a result of the first monitoring, second monitoring a second transfer rate of second read data during another of the read procedures, and further determining whether an anomaly region is present in the data segment based on the monitored second transfer rate.

5. (Previously Presented) The method of claim 1 wherein calculating corresponding digital signatures for each of the multiple read data results comprises calculating a digital signature selected from the group consisting of message digest algorithm 2 (MD2), message digest algorithm 4 (MD4), message digest algorithm 5 (MD5), Snefru, secure hash algorithm (SHA), National Institute of Standards and Technology digital signature algorithm (NIST DSA), Haval, N-Hash, and RACE integrity primitives evaluation message digest (RIPE-MD) digital signatures.

6. (Cancelled)

7. (Original) The method of claim 6 further comprising, if none of the digital signatures are equal in value, determining the anomaly region to be present.

8. (Cancelled)

9. (Cancelled)

10. (Previously Presented) A system for authenticating a digital medium by determining the presence of an anomaly region corresponding to a data segment of the digital medium comprising:

a read unit for performing multiple read operations on a data segment of the medium to generate multiple corresponding read data results;

a calculating unit for calculating corresponding digital signatures using actual data values of underlying data of the read data segment for each of the multiple read data results; and

a determining unit for determining whether an anomaly region is present in the data segment based on a comparison of the digital signatures by determining whether any of the digital signatures are equal in value, and if a predetermined number of the digital signatures are not equal in value, the determining unit determining the anomaly region to be present; and

a means for authenticating the medium in response to the determination of the presence of the anomaly region.

11. (Original) The system of claim 10 wherein the data comprises data selected from the group consisting of: user data, error data, sync data, parity data, header data, and sub-channel data.

12. (Original) The system of claim 10 further comprising a rate monitoring unit for monitoring a transfer rate of the read data during at least one of the read procedures, and further determining whether an anomaly region is present in the data segment based on the monitored transfer rate.

13. (Original) The system of claim 10 further comprising:

a monitoring unit for first monitoring a first transfer rate of first read data during one of the read procedures, and further determining whether an anomaly region is present in the data segment based on the monitored first transfer rate; and, in the event that the presence of an anomaly is not determined as a result of the first monitoring, second monitoring a second transfer rate of second read data during another of the read procedures, and further determining whether an anomaly region is present in the data segment based on the monitored second transfer rate.

14. (Previously Presented) The system of claim 10 wherein the calculating unit calculates a digital signature selected from the group consisting of message digest

algorithm 2 (MD2), message digest algorithm 4 (MD4), message digest algorithm 5 (MD5), Snefru, secure hash algorithm (SHA), National Institute of Standards and Technology digital signature algorithm (NIST DSA), Haval, N-Hash, and RACE integrity primitives evaluation message digest (RIPE-MD) digital signatures.

15. (Cancelled)

16. (Original) The system of claim 15 wherein, if none of the digital signatures are equal in value, the anomaly region is determined to be present.

17. (Cancelled)

18. (Cancelled)